

CLAIMS

We claim:

- 1 1. A method of operating an intrusion detection system, the method comprising the steps of:
 - 2 determining a present alert generation rate of an intrusion detection system;
 - 3 comparing the present alert generation rate with an alert generation rate threshold; and
 - 4 altering an element of a signature set of the intrusion detection system responsive to an
 - 5 outcome of the step of comparing.
- 1 2. A method of operating an intrusion detection sensor, the method comprising the steps of:
 - 2 determining a present alert generation rate of an intrusion detection sensor;
 - 3 comparing the present alert generation rate with an alert generation rate threshold; and
 - 4 when the present alert generation rate exceeds the alert generation rate threshold, altering
 - 5 an element of a signature set of the intrusion detection sensor to decrease an alert generation rate
 - 6 of the intrusion detection sensor.

1 3. The method of claim 2, wherein the element is a signature threshold quantity.

1 4. The method of claim 2, wherein the element is a signature threshold interval.

1 5. A method of operating an intrusion detection system, comprising the steps of:

2 monitoring for occurrence of a signature event; and

3 when a signature event occurs, increasing a value of a signature event counter and

4 comparing the value of the signature event counter with a signature threshold quantity; and

5 when the value of the signature event counter exceeds the signature threshold quantity,

6 generating an alert, recording a time of generating the alert in a log, determining from contents of

7 the log a present alert generation rate, and comparing the present alert generation rate with an

8 alert generation rate threshold; and

9 when the present alert generation rate exceeds the alert generation rate threshold, altering

10 an element of a signature set of an intrusion detection system to decrease an alert generation rate

11 of an intrusion detection sensor.

1 6. The method of claim 5, wherein the element is a signature threshold quantity.

1 7. The method of claim 5, wherein the element is a signature threshold interval.

1 8. Programmable media containing programmable software for operation of an intrusion
2 detection system, programmable software comprising the steps of:

3 determining a present alert generation rate of an intrusion detection system;

4 comparing the present alert generation rate with an alert generation rate threshold; and

5 altering an element of a signature set of the intrusion detection system responsive to an
6 outcome of the step of comparing.

1 9. Programmable media containing programmable software for operation of an intrusion
2 detection sensor, programmable software comprising the steps of:

3 determining a present alert generation rate of an intrusion detection sensor;

4 comparing the present alert generation rate with an alert generation rate threshold; and

5 when the present alert generation rate exceeds the alert generation rate threshold, altering
6 an element of a signature set of the intrusion detection sensor to decrease an alert generation rate
7 of the intrusion detection sensor.

1 10. Programmable media containing programmable software for operation of an intrusion
2 detection system, programmable software comprising the steps of:

3 monitoring for occurrence of a signature event; and

4 when a signature event occurs, increasing a value of a signature event counter and
5 comparing the value of the signature event counter with a signature threshold quantity; and

6 when the value of the signature event counter exceeds the signature threshold quantity,
7 generating an alert, recording a time of generating the alert in a log, determining from contents of
8 the log a present alert generation rate, and comparing the present alert generation rate with an
9 alert generation rate threshold; and

10 when the present alert generation rate exceeds the alert generation rate threshold, altering
11 an element of a signature set of an intrusion detection system to decrease an alert generation rate
12 of an intrusion detection server.

